establish additional requirements based on the sensitivity of the particular, identified categories of classified information necessary to perform the lawful and authorized functions that are the basis for granting temporary eligibility for access. However, no additional requirements shall exceed the common standards for background investigations developed under section 3.2(b) of Executive Order 12968. Temporary eligibility for access is valid only at the agency granting it and at other agencies who expressly agree to accept it and acknowledge understanding of its investigative basis. It is further subject to limitations specified in sections 2.4(d) and 3.3 of Executive Order 12968, *Access to Classified Information*.

PART 148—NATIONAL POLICY AND IMPLEMENTATION OF RECIPROCITY OF FACILITIES

Subpart A—National Policy on Reciprocity of Use and Inspections of Facilities

Subpart B—Guidelines for the Implementation and Oversight of the Policy on Reciprocity of Use and Inspections of Facilities

AUTHORITY: E.O. 12968 (60 FR 40245, 3 CFR 1995 Comp., p. 391.)

SOURCE: 63 FR 4580, Jan. 30, 1998, unless otherwise noted.

Subpart A—National Policy on Reciprocity of Use and Inspections of Facilities

§ 148.1 Intergency reciprocal acceptance .

Interagency reciprocal acceptance of security policies and procedures for approving, accrediting, and maintaining the secure posture of shared facilities will reduce aggregate costs, promote interoperability of agency security systems, preserve vitality of the U.S. industrial base, and advance national security objectives.

§ 148.2 Classified programs.

Once a facility is authorized, approved, certified, or accredited, all U.S. Government organizations desiring to conduct classified programs at the facility at the same security level shall accept the authorization, approval, certification, or accreditation without change, enhancements, or upgrades. Executive Order, Safeguarding Directives, National Industrial Security Program Operating Manual (NISPOM), the NISPOM Supplement, the Director of Central Intelligence Directives, interagency agreements, successor documents, or other mutually agreed upon methods shall be the basis for such acceptance.

§ 148.3 Security review.

After initial security authorization, approval, certification, or accreditation, subsequent security reviews shall normally be conducted no more frequently than annually.

Additionally, such reviews shall be aperiodic or random, and be based upon risk management principles. Security reviews may be conducted ''for cause'', to follow up on previous findings, or to accomplish close-out actions. Visits may be made to a facility to conduct security support actions, administrative inquiries, program reviews, and approvals as deemed appropriate by the cognizant security authority or agency.

§ 148.4 Policy documentation.

Agency heads shall ensure that any policy documents their agency issues setting out facilities security policies and procedures incorporate the policy set out herein, and that such policies are reasonable, effective, efficient, and enable and promote interagency reciprocity.

§ 148.5 Idenfification of the security policy board.

Agencies which authorize, approve, certify, or accredit facilities shall provide to the Security Policy Board Staff a points of contact list to include names and telephone numbers of personnel to be contacted for verification of authorized, approved, certified, or accredited facility status. The Security Policy Board Staff will publish a comprehensive directory of points of contact.

§ 148.6 Agency review.

Agencies will continue to review and assess the potential value added to the process of co-use of facilities by development of electronic data retrieval across government. As this review continues, agencies creating or modifying facilities databases will do so in a manner which facilitates community data sharing, interest of national defense or foreign policy.

Subpart B—Guidelines for the Implementation and Oversight of the Policy on Reciprocity of use and Inspections of Facilities

§ 148.10 General.

(a) Redundant, overlapping, and duplicative policies and practices that govern the co-use of facilities for classified purposes have resulted in excessive protection and unnecessary expenditure of funds. Lack of reciprocity has also impeded achievement of national security objectives and adversely affected economic and technological interest.

(b) Interagency reciprocal acceptance of security policies and procedures for approving, accrediting, and maintaining the secure posture of shared facilities will reduce the aggregate costs, promote interoperability of agency security systems, preserve the vitality of the U.S. industrial base, and advance national security objectives.

(c) Agency heads, or their designee, are encouraged to periodically issue written affirmations in support of the policies and procedures prescribed herein and in the Security Policy Board (SPB) policy, entitled ''Reciprocity of Use and Inspections of Facilities.''

(d) The policies and procedures prescribed herein shall be applicable to all agencies. This document does not supersede the authority of the Secretary of Defense under Executive Order 12829 (58 FR 3479, 3 CFR 1993 Comp., p. 570); the Secretary of Energy or the Chairman of the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended; the Secretary of State under the Omnibus Diplomatic Security and Anti-Terrorism Act of 1986; the Secretaries of the military departments and military department installation Commanders under the Internal Security Act of 1950; the Director of Central Intelligence under the National Security Act of 1947, as amended, or Executive Order 12333; the Director of the Information Security Oversight Office under Executive Order 12829 or Executive Order 12958 (60 FR 19825, 3 CFR 1995 Comp., p. 333); or substantially similar authority instruments assigned to any other agency head.

§ 148.11 Policy.

(a) Agency heads, or their designee, shall ensure that security policies and procedures for which they are responsible are reasonable, effective, and efficient, and that those policies and procedures enable and promote interagency reciprocity.

(b) To the extent reasonable and practical, and consistent with US law, Presidential decree, and bilateral and international obligations of the United States, the security requirements, restrictions, and safeguards applicable to industry shall be equivalent to those applicable within the Executive Branch of government.

(c) Once a facility is authorized approved, certified, or accredited, all government organizations desiring to conduct classified programs at the facility at the same security level shall accept the authorization, approval, certification, or accreditation without change, enhancements, or upgrades.

§ 148.12 Definitions.

Agency. Any ''executive agency,'' as defined in 5 U.S.C. 105; any ''Military department'' as defined in 5 U.S.C. 102;

and any other entity within the Executive Branch that comes into possession of classified information.

Classified Information. All information that requires protection under Executive Order 12958, or any of its antecedent orders, and the Atomic Energy Act of 1954, as amended.

Cognizant Security Agency (CSA). Those agencies that have been authorized by Executive Order 12829 to establish an industrial security program for the purpose of safeguarding classified information disclosed or released to industry.

Cognizant Security Office (CSO). The office or offices delegated by the head of a CSA to administer industrial security in a contractor's facility on behalf of the CSA.

Facility. An activity of a government agency or cleared contractor authorized by appropriate authority to conduct classified operations or to perform classified work.

Industry. Contractors, licensees, grantees, and certificate holders obligated by contract or other written agreement to protect classified information under the National Industrial Security Program.

National Security. The national defense and foreign relations of the United States.

Senior Agency Official. Those officials, pursuant to Executive Order 12958, designated by the agency head who are assigned the responsibility to direct and administer the agency's information security program.

§ 148.13 Responsibilities.

(a) Each Senior Agency Official shall ensure that adequate reciprocity provisions are incorporated within his or her regulatory issuances that prescribe agency safeguards for protecting classified information.

(b) Each Senior Agency Official shall develop, implement, and oversee a program that ensures agency personnel adhere to the policies and procedures prescribed herein and the reciprocity provisions of the National Industrial Security Program Operating Manual (NISPOM).

(c) Each Senior Agency Official must ensure that implementation encourages reporting of instances of non-compliance, without fear of reprisal, and each reported instance is aggressively acted upon.

(d) The Director, Information Security Oversight Office (ISOO), consistent with his assigned responsibilities under Executive Order 12829, serves as the central point of contact within Government to consider and take action on complaints and suggestions from industry concerning alleged violations of the reciprocity provisions of the NISPOM.

(e) The Director, Security Policy Board Staff (D/SPBS) or his/her designee, shall serve as the central point of contact within Government to receive from Federal Government employees alleged violations of the reciprocity provisions prescribed herein and the policy ''Reciprocity of Use and Inspections of Facilities'' of the SPB.

§ 148.14 Procedures.

(a) Agencies that authorize, approve, certify, or accredit facilities shall provide to the SPB Staff a points of contact list to include names and telephone numbers of personnel to be contacted for verification of the status of facilities. The SPB Staff will publish a comprehensive directory of agency points of contact.

(b) After initial security authorization, approval, certification, or accreditation, subsequent reviews shall normally be conducted no more frequently than annually. Additionally, such reviews shall be aperiodic or random, and be based upon risk-management principles. Security Reviews may be conducted ''for cause'', to follow up on previous findings, or to accomplish closeout actions.

(c) The procedures employed to maximize interagency reciprocity shall be based primarily upon existing organizational reporting channels. These channels should be used to address alleged departures from established reciprocity requirements and should resolve all, including the most egregious instances of non-compliance.

(d) Two complementary mechanisms are hereby established to augment existing organizational channels: (1) An accessible and responsive venue for reporting and resolving complaints/reported instances of non-compliance.

Government and industry reporting channels shall be as follows:

(1) *Governnment.* (A) Agency employees are encouraged to bring suspected departures from applicable reciprocity requirements to the attention of the appropriate security authority in accordance with established agency procedures.

(B) Should the matter remain unresolved, the complainant (employee, Security Officer, Special Security Officer, or similar official) is encouraged to report the matter formally to the Senior Agency Official for resolution.

(C) Should the Senior Agency Official response be determined inadequate by the complainant, the matter should be reported formally to the Director, Security Policy Board Staff (D/SPBS). The D/SPBS, may revisit the matter with the Senior Agency Official or refer the matter to the Security Policy Forum as deemed appropriate.

(D) Should the matter remain unresolved, the Security Policy Forum may consider referral to the SPB, the agency head, or the National Security Council as deemed appropriate.

(ii) *Industry.* (A) Contractor employees are encouraged to bring suspected departures from the reciprocity provisions of the NISPOM to the attention to their Facility Security Officer (FSO) or Contractor Special Security Officer (CSSO), as appropriate, for resolution.

(B) Should the matter remain unresolved, the complainant (employee, FSO, or CSSO) is encouraged to report the matter formally to the Cognizant Security Office (CSO) for resolution.

(C) Should the CSO responses be determined inadequate by the complainant, the matter should be reported formally to the Senior Agency Official within the Cognizant Security Agency (CSA) for resolution.

(D) Should the Senior Agency Official response be determined inadequately by the complainant, the matter should be reported formally to the Director, information Security Oversight Office (ISOO) for resolution.

(E) The Director, ISOO, may revisit the matter with the Senior Agency Official or refer the matter to the agency head or the National Security Council as deemed appropriate.

(2) An annual survey administered to a representative sampling of agency and private sector facilities to assess overall effectiveness of agency adherence to applicable reciprocity requirements.

(i) In coordination with the D/SPBS, the Director, ISOO, as Chairman of the NISP Policy Advisory Committee (NISPPAC), shall develop and administer an annual survey to a representative number of cleared contractor activities/employees to assess the effectiveness of interagency reciprocity implementation. Administration of the survey shall be coordinated fully with each affected Senior Agency Official.

(ii) In coordination with the NISPPAC, the D/SPBS shall develop and administer an annual survey to a representative number of agency activities/personnel to assess the effectiveness of interagency reciprocity implementation. Administration of the survey shall be coordinated fully with each affected Senior Agency Official.

(iii) The goal of annual surveys should not be punitive but educational. All agencies and departments have participated in the crafting of these facilities policies, therefore, non-compliance is a matter of internal education and direction.

(e) Agencies will continue to review and assess the potential value added to the process of co-use of facilities by development of electronic data retrieval across government.

PART 149—POLICY ON TECHNICAL SURVEILLANCE COUNTERMEASURES

Sec.
149.1 Policy.
149.2 Responsibilities.
149.3 Definitions.

AUTHORITY: E.O. 12968 (60 FR 40245, 3 CFR 1995 Comp., p. 391.)

SOURCE: 63 FR 4583, Jan. 30, 1998, unless otherwise noted.

§ 149.1 Policy.

(a) Heads of federal departments and agencies which process, discuss, and/or store classified national security information, restricted data, and sensitive but unclassified information, shall, in response to specific threat data and based on risk management principles,